Video Server

VS3100P

User's Manual

Product name:	Video Server (VS3100P)
Release Date:	2005/04/07
Manual Revision:	1.30
Web site:	www.vivotek.com
Email:	technical@vivotek.com
	sales@vivotek.com
Made in Taiwan.	©Copyright 2000-2005. All rights reserved

Before You Use This Product

The use of surveillance devices may be prohibited by law in your country. The Video Server is not only a high-performance web-ready camera but also can be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

It is important to first verify that all contents received are complete according to the list in the "Package Contents" chapter. Take notice of the warnings in "Quick installation guide" before the Video Server is installed, then carefully read and follow the instructions in the "Installation" chapter to avoid damages due to faulty assembly and installation. This also ensures the product is used properly as intended.

The Video Server is a network device and its use should be straightforward for those who have basic network knowledge. The "Troubleshooting" chapter in the Appendix provides remedies to the most common errors in set up and configuration. You should consult this chapter first if you run into a system error.

The Video Server is designed for various applications including video sharing, general security/surveillance, etc. The "How to Use" chapter suggests ways to best utilize the Video Server and ensure proper operations. For the creative and professional developers, the "URL Commands of The Video Server " chapter serves to be a helpful reference to customize existing homepages or integrating with the current web server.

For paragraphs preceded by ⚠ the reader should use caution to understand completely the warnings. Ignoring the warnings may result in serious hazards or injuries.

Table of Contents

Package Contents

VS3100P

Software CD

Power adapter

Quick installation guide

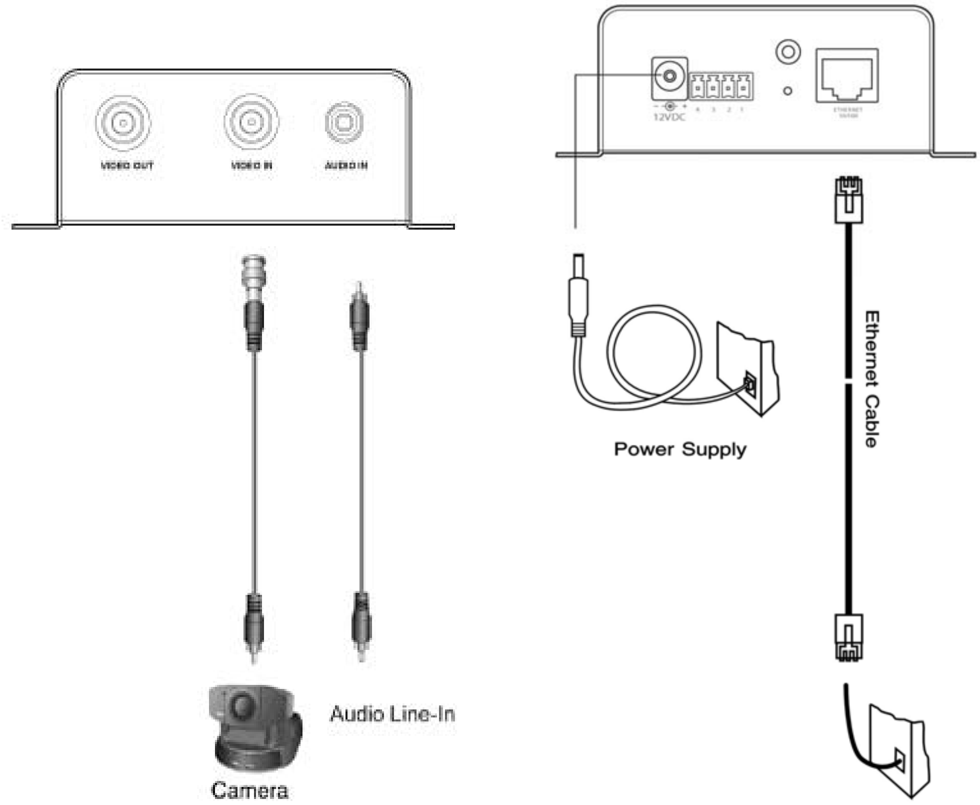
I/O terminal block connector

Warranty card

HARDWARE LIMITED WARRANTY

[illegible]

Physical Description



Front Panel

BNC video input

75Ohms resistance video port for connecting an external camera. To ensure video modulation type being correctly detected, cameras should be attached and powered on before the Video Server is powered on.

BNC video output

Bypass the video input signal to additional terminal or surveillance equipment.

RCA audio input

The audio input is connected by RCA connector of mono-audio Line-In signal.

Status LED

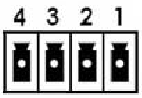
The Video Server provides a LED to show its status. Please refer to the appendix "Troubleshooting” for detail.

Rear Panel

Ethernet 10/100 socket

Connect to Ethernet network with a UTP category 5 cable that cannot exceed 100 meters.

General I/O terminal block

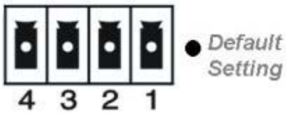


1	DI-	INPUT (Initial state of DI is low)
2	DI+	INPUT (Max. 50mA, 12VDC)
3	SW_COMMON	OUTPUT (open from SW_OPEN at initial state) (close with SW_OPEN when set DO to ON)
4	SW_NOPEN	OUTPUT (Max. 1A, 24VDC or 0.5A, 125VAC)

The Video Server provides a general I/O terminal block with one digital input and one relay switch for device control. Pin 1 and pin 2 can be connected to an external sensor device and the state of voltage will be monitored from the initial state 'LOW'. The relay switch of pin 3 and pin 4 can be used to turn on or off the external device.

⚠ Consult with the dealer of the peripherals for correct installation.

Restore button



There is a button hidden in the box for restoring the system factory default settings. Please refer to the appendix "Troubleshooting" for detail.

Power adapter

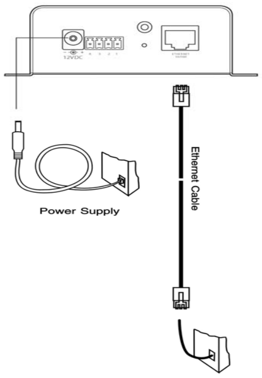
Connect the power jack of the included power adapter. Connecting the power adapter should be the last operation while physically installing the Video Server.

Installation

Hardware installation

Before installing multiple Video Servers at the well-chosen locations, the Administrator should memorize the serial numbers on the packages respectively for future use.

Cable connection



Shut down all the peripheral devices prior to connection. Connect the supplied cables from the Video Server to related devices according to the figure. The Ethernet cable should meet UTP category 5 that cannot exceed 100 meters.

Power on

Make sure all cables are correctly and firmly connected before turning on the Video Server. Turn on cameras, sensors, alarm devices, and then attach the power adaptor of the Video Server to the electric power socket. As soon as the power adapter is plugged into the utility socket, the front LED will switch between green and red for several times. After passing the self-test, the LED will be green and the Video Server will standby for getting IP address. After getting IP Address, the LED will blink green every second. Otherwise refer to Appendix A for troubleshooting.

⚠ Connect the jack of the power adapter to Video Server prior to plugging the utility end into the utility power socket. It will reduce accidental electric surge shock.

Software installation

At the end of the hardware installation, users can use Installation Wizard program included in the product CDROM to find the location of the Video Server. There may be many Video Servers in the local network. Users can differentiate the Video Servers with the serial number. The serial number is printed on the labels on the carton and the back of the Video Server body. Please refer to the user’s manual of Installation Wizard for detail.

Once installation is complete, the Administrator should proceed to the next section "Initial access to the Video Server" for necessary checks and configurations.

Initial Access to the Video Server

Check Network Settings

The Video Server can be connected either before or immediately after software installation onto the Local Area Network. The Administrator should complete the network settings on the configuration page, including the correct subnet mask and IP address of gateway and DNS. Ask your network administrator or Internet service provider for the detail information. By default the Video Server requires the Administrator to run installation every time it reboots. If the network settings are to remain unchanged, disable the Install option. Refer to “Network settings” on the System Configuration page for details. If any setting is entered incorrectly and cannot proceed to setting up the Video Server, restore the factory settings following the steps in the “Troubleshooting” chapter of the Appendix.

Add Password to prevent Unauthorized Access

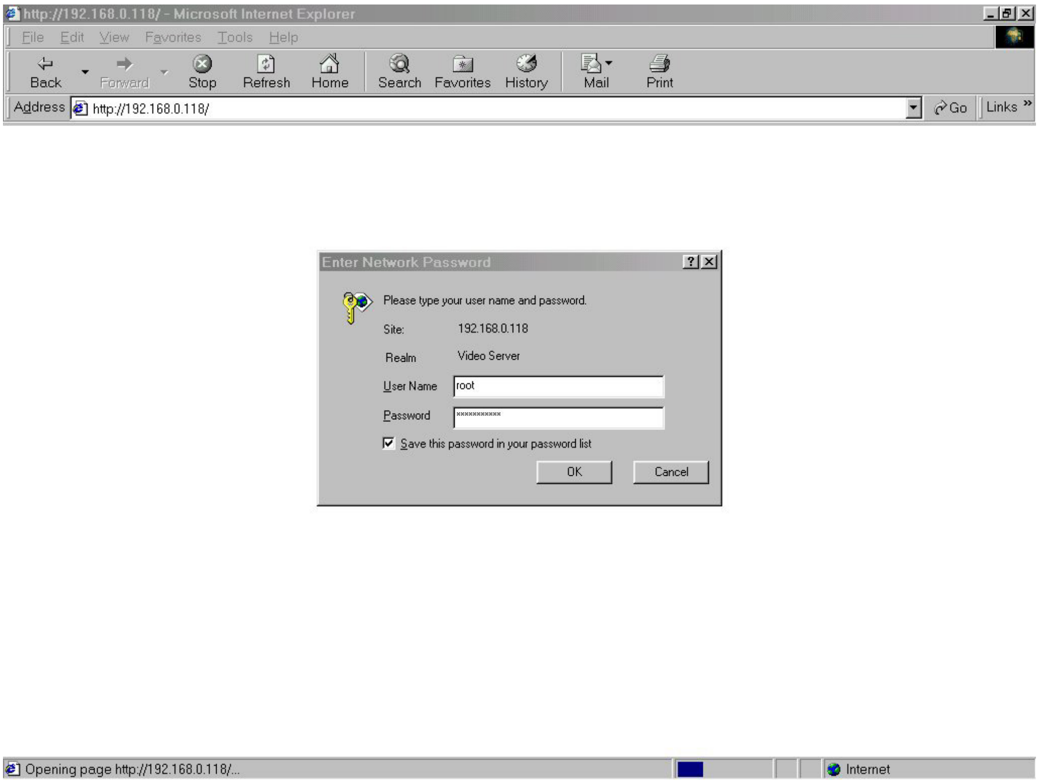
The default Administrator’s password is blank and the Video Server initially will not ask for any password. The Administrator should immediately implement a new password as a matter of prudent security practice. Once the Administrator’s password is saved, the Video Server will ask for the user’s name and password before each access. The Administrator can set up a maximum of twenty (20) user accounts. Each user can access the Video Server except to perform system configuration. Some critical functions are exclusive for the Administrator, such as system configuration, user administration, and software upgrades. The user name for the Administrator is permanently assigned as “root”. Once the password is changed, the browser will display an authentication window to ask for the new password. **Once the password is set, there is no provision to recover the Administrator’s password. The only option is to restore to the original factory default settings.**

How to Use

Authentication

After opening the Web browser and typing in the URL of the Video Server, a dialogue window pops up to request a username and password. Upon successful authentication, the following figure is displayed.

The foreground is the login window and the background shows the message if authentication fails. The user may check the option box to save the password for future convenience. This option is not available to the Administrator for obvious reason.



Address: http://192.168.0.118/

Please type your user name and password.

Site: 192.168.0.118

Realm: Video Server

User Name: root

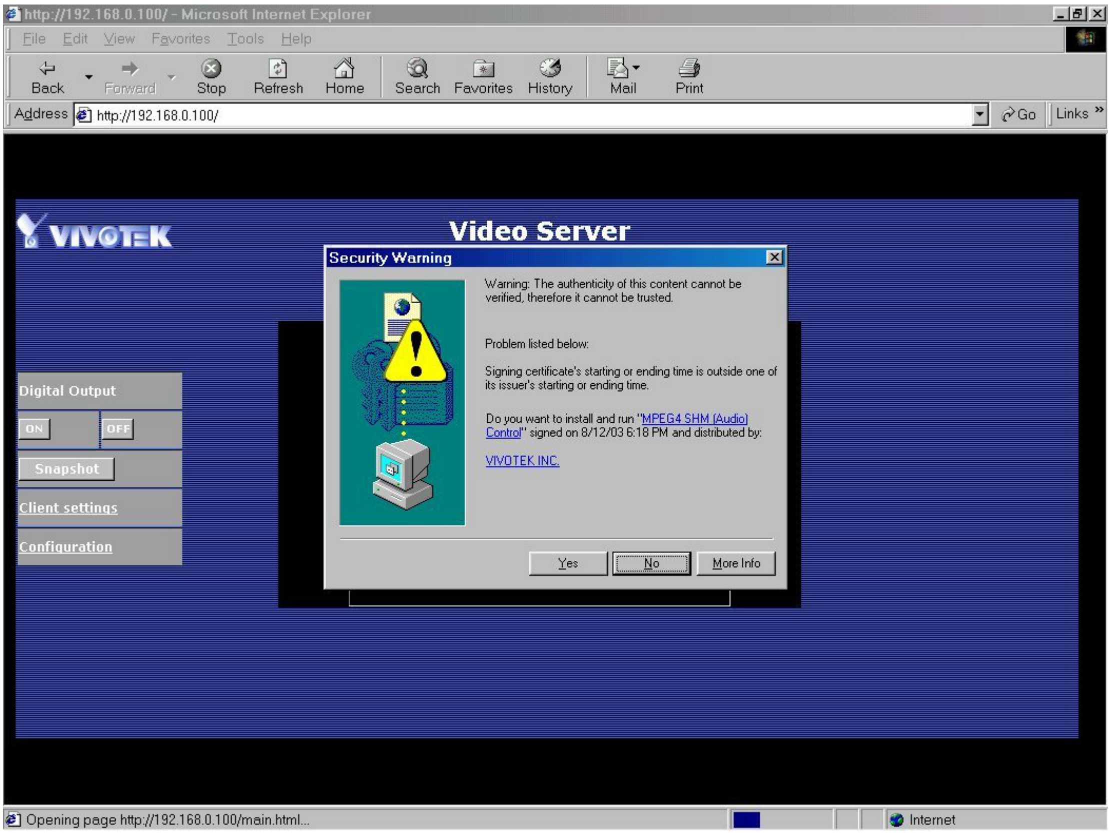
Password: ***********

☑ Save this password in your password list

Opening page http://192.168.0.118/...

Installing plug-in

For the initial access to the Video Server in Windows, the web browser may prompt for permission to install a new plug-in for the Video Server. Permission request depends on the Internet security settings of the user's PC or notebook. If the highest security level is set, the computer may prohibit any installation and execution attempt. This plug-in has been registered for certificate and is used to display the video in the browser. Users may click on Yes to proceed. If the web browser does not allow the user to continue to install, check the Internet security option and lower the security levels or contact your IT or networking supervisor for help.



Warning: The authenticity of this content cannot be verified, therefore it cannot be trusted.

Problem listed below:

Signing certificate's starting or ending time is outside one of its issuer's starting or ending time.

Do you want to install and run "MPEG4 SHM (Audio) Control" signed on 8/12/03 6:18 PM and distributed by:

VIVOTEK INC.

Opening page http://192.168.0.100/main.html...

Primary user's capability

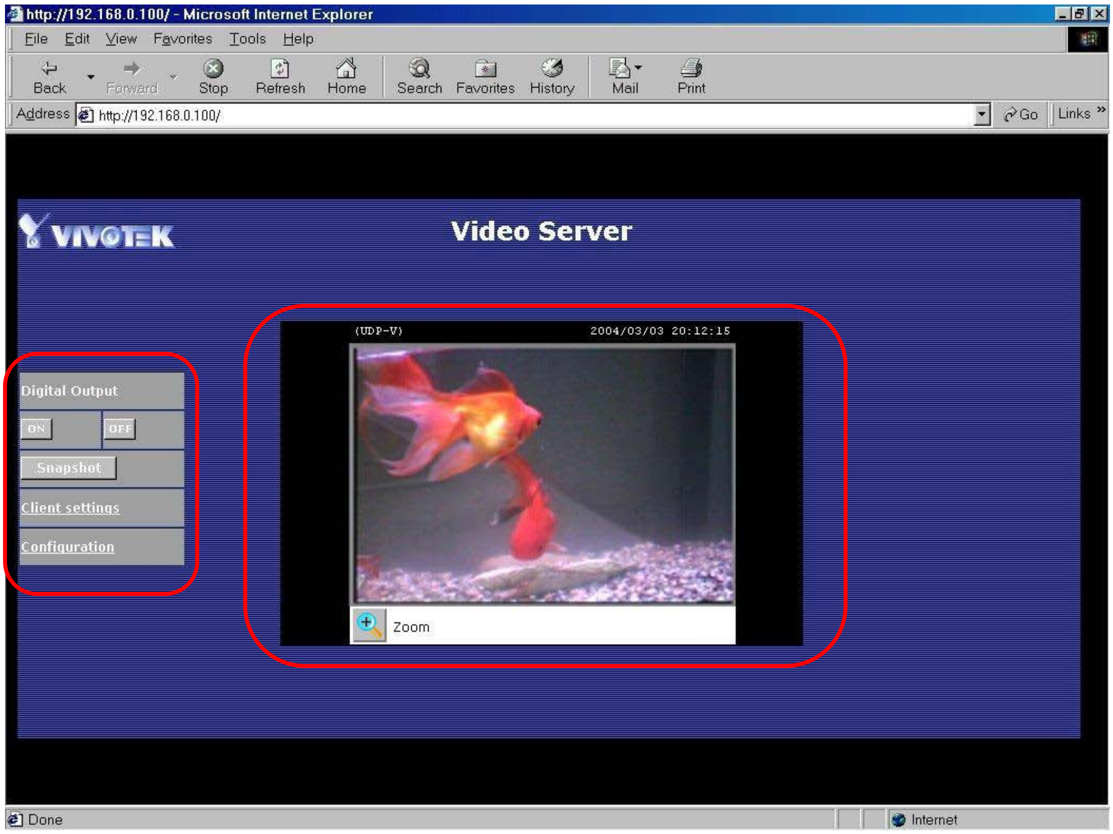
Main Screen with Camera View

The main page layout has two parts:

Configuration functions: The camera can be configured using these user interfaces.

Camera View: What the camera sees.

Click on the configuration link to the left of the image window to enter the configuration page.


http://192.168.0.100/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.0.100/
Go Links
Video Server
Digital Output
ON OFF
Snapshot
Client settings
Configuration
(UDP-V)
2004/03/03 20:12:15
Zoom
Done
Internet

Digital Zoom

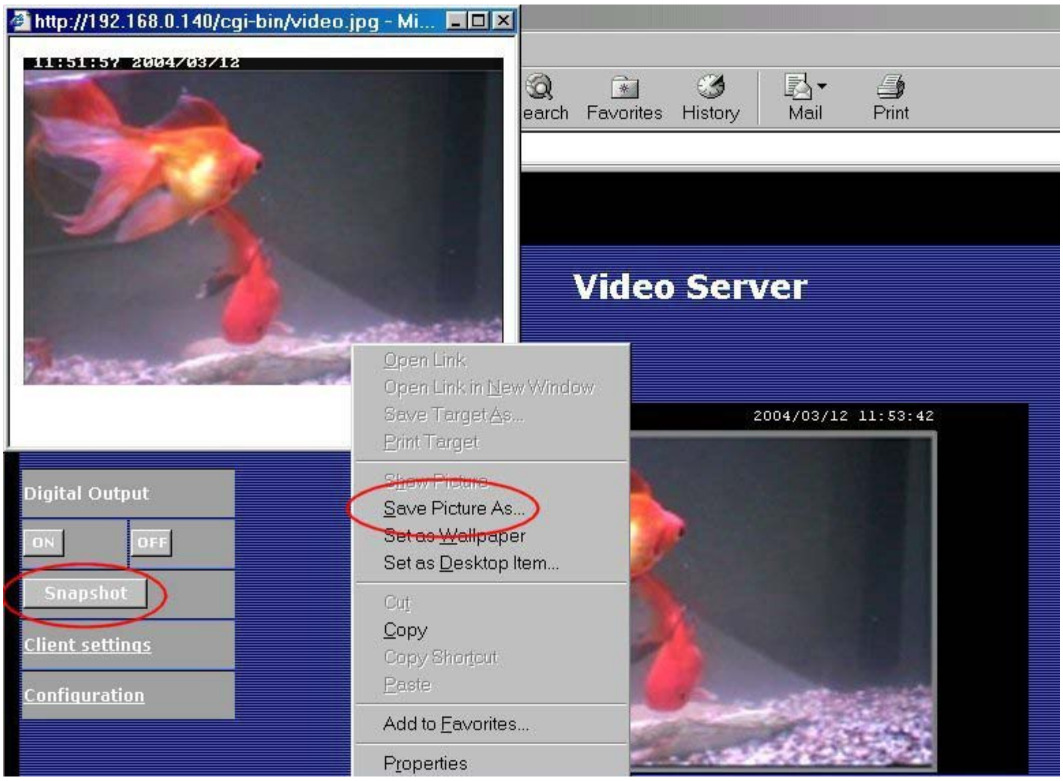
Click on the magnifier icon under the camera view then the digital zoom control panel will be shown. Uncheck “Disable digital zoom” and use the slider control to change the zoom factors.

Digital Output

Clicking on the “On” or “Off” button turns the digital output to either on or off status.

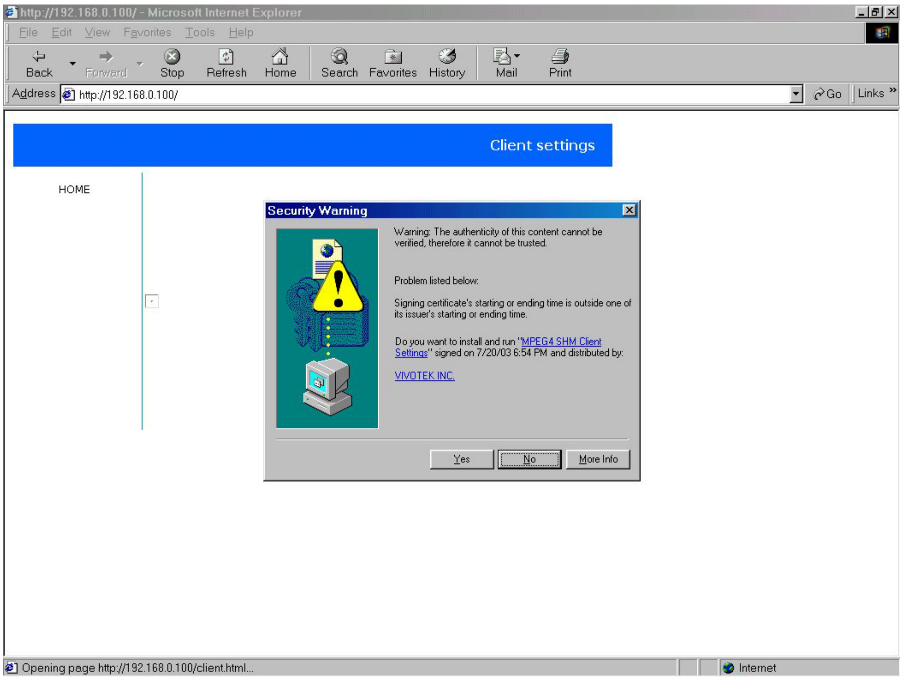
Snapshot

Click on Snapshot, web browser will pop up a new window to show the snapshot. Users can point at the snapshot and click the right button of mouse to save it.



Client settings

At the initial access to the “Connection type” page in Windows, the web browser will ask for a new plug-in installation, the plug-in being the Video Server. This plug-in has been registered for certification and can be used to change the parameters at the client’s site. The user may click on Yes to install the plug-in. If the web browser does not allow the user to complete the installation, check the Internet security to lower the security level or contact your IT or networking supervisor.


http://192.168.0.100/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Forward
Stop
Refresh
Home
Search
Favorites
History
Mail
Print
Address http://192.168.0.100/
Go
Links
Client settings
HOME
Yes
No
More Info
Opening page http://192.168.0.100/client.html...
Internet

Security Warning

Warning: The authenticity of this content cannot be verified, therefore it cannot be trusted.

Problem listed below:

Signing certificate's starting or ending time is outside one of its issuer's starting or ending time.

Do you want to install and run "MPEG4 SHM Client Settings" signed on 7/20/03 6:54 PM and distributed by:

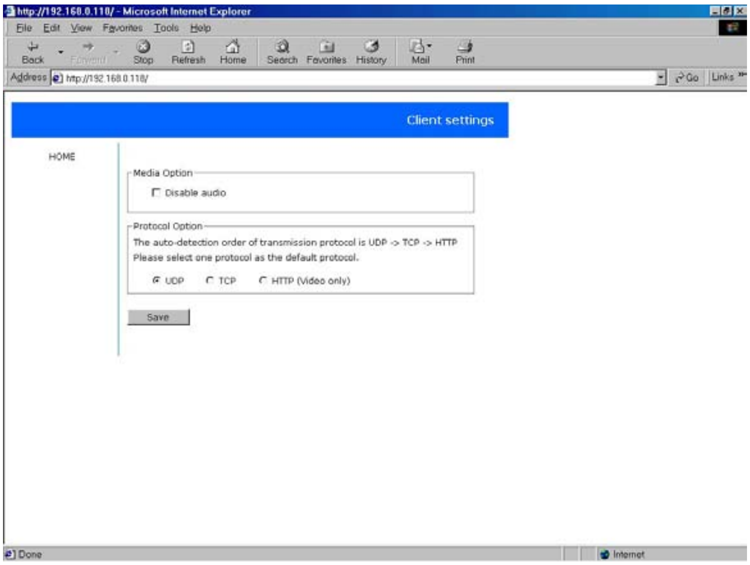
VIVOTEK INC.

There are two settings for the client side. One is “**Media Option**” for users to determine if audio should be muted. The other is “**Protocol Option**” which allows choices on connection protocol between client and server. There are three protocols choices to optimize your usage - UDP, TCP and HTTP.

The **UDP** protocol allows for more real-time audio and video streams. However, some packets may be lost due to network burst traffic and images may be obscured.

The **TCP** protocol allows for less packet loss and produces a more accurate video display. The downside with this protocol is that the real-time effect is worse than that with the UDP protocol.

The **HTTP** protocol must be selected if the network is protected by a firewall and it only allows HTTP Port (80) to be opened. In this mode, audio will not be sent and only video is operational. If no special need is required, UDP protocol is recommended. Generally speaking, the client's choice will be in the order of UDP → TCP → HTTP. After the Video Server is connected successfully, "Protocol Option" will indicate the selected protocol. The selected protocol will be recorded in the user's PC and will be used for the next connection. If the network environment is changed, or the user wants to let the web browser to detect again, manually select the UDP protocol, save, and return HOME to re-connect.


http://192.168.0.118/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.0.118/
Go Links
Done
Internet

Client settings

HOME

Media Option

□ Disable audio

Protocol Option

The auto-detection order of transmission protocol is UDP -> TCP -> HTTP
Please select one protocol as the default protocol.

● UDP ○ TCP ○ HTTP (Video only)

Save

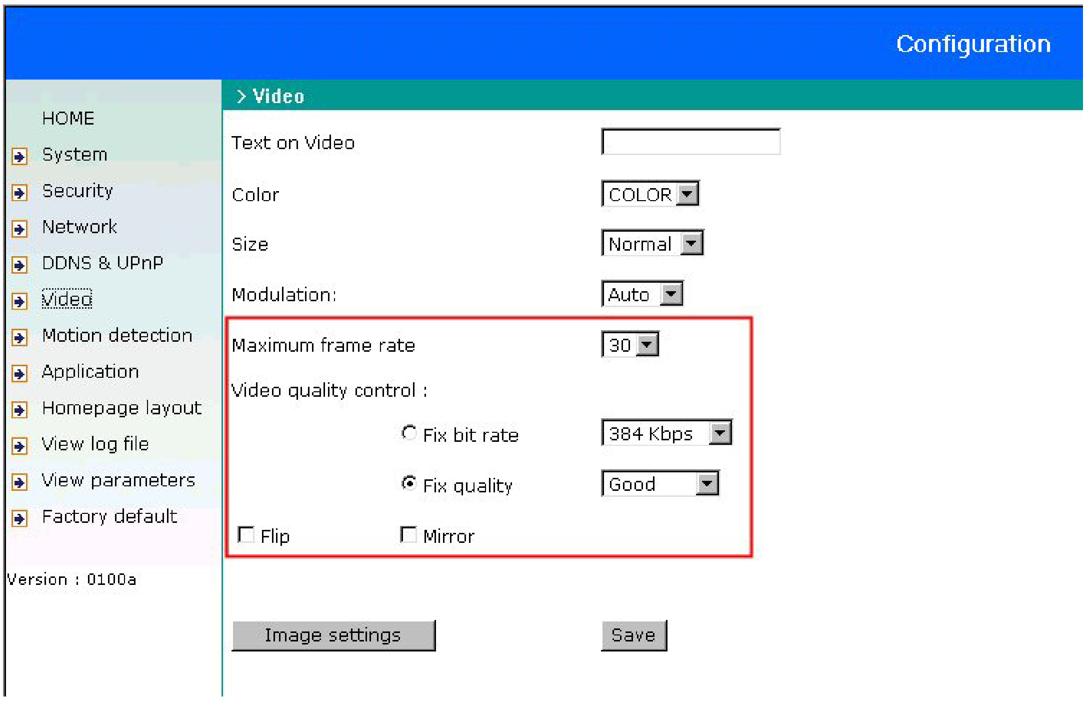
<url> *http://<Video Server>/protocol.html*

<Video Server> is the domain name or the original IP address of the Video Server.

Administrator’s capability

Fine-tuning for Best Performance

Best performance generally equates to the fastest image refresh rate with the best video quality, and at the lowest network bandwidth as possible. The three factors, “Maximum frame rate”, “Fix bit rate”, and “Fix quality” on the Video Configuration page, are correlative to allow for achieving the best performance possible.



> Video

Text on Video

Color: COLOR

Size: Normal

Modulation: Auto

Maximum frame rate: 30

Video quality control :

○ Fix bit rate: 384 Kbps

● Fix quality: Good

□ Flip □ Mirror

For Best Real-time Video Images

To achieve good real-time visual effect, the network bandwidth should be large enough to allow a transmission rate of greater than 20 image frames per second. If the broadband network is over 1 Mbps, set the “Fix bit rate” to 1000Kbps or 1200Kbps, and set “Fix quality” at the highest quality. The maximum frame rate is 25 in PAL system and 30 in NTSC system. If your network bandwidth is more than 384Kbps, you can fix the bit rate according to your bandwidth and set the maximum frame rate to 25 fps or 30 fps. If the images vary dramatically in your environment, you may want to slow the maximum frame rate down to 20 fps in order to lower the rate of data transmission. This allows for better video quality and the human eyes cannot readily detect the differences between those of 20, 25, or 30 frames per second. If your network bandwidth is below 384 Kbps, set the “Fix bit rate” according to your bandwidth and try to get the best performance by fine-tuning with the “Maximum frame rate”. In a slow network, greater frame rate results in blur images. Another work-around is to choose “Half” in the “Size” option for better images, or “Halfx2” for a larger image view. Video quality performance will vary somewhat due to the number of users viewing on the network; even when the parameters have initially been finely tuned. Performance will also suffer due to poor connectivity because of the network’s burst constraint.

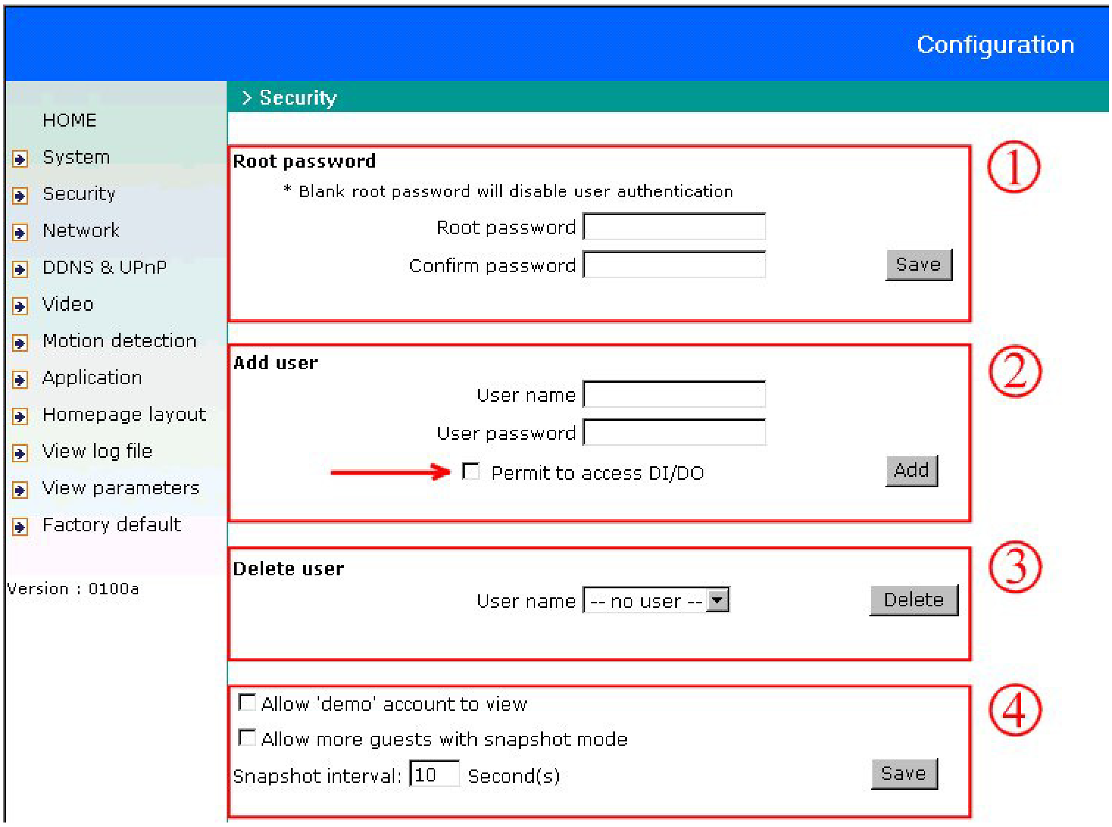
Only Quality Images Will Do

To have the best video quality, you should set “Fix quality” at “Detailed” or “Excellent” and adjust the “Maximum frame rate” to match your network’s bandwidth. If your network is slow and you receive “broken” pictures, go to the TCP protocol in “Connection type” and choose a more appropriate mode of transmission. The images may suffer a time delay due to a slower connection. The delay will also increase with added number of users.

Somewhere Between Real-time and Clear Images

If you have a broadband network, set “Fix quality” at ”Normal” or better, rather than setting “Fix bit rate”. You can also fix the bandwidth according to your actual network speed and adjust the frame rate. Start from 30 fps down for best results but not below 15 fps. If the image qualities are not improved, select a lower bandwidth setting.

Opening accounts for new users



* Blank root password will disable user authentication

Protect Video Server by passwords

The Video Server is shipped without any password by default. That means everyone can access the Video Server including the configuration as long as the IP address is known. It is necessary to assign a password if the Video Server is intended to be accessed by others. Type a new word twice in ① to enable protection. This password is used to identify the administrator. Then add an account with user name and password for your friends in ②. Video Server can provide twenty accounts for your valuable customers or friends. Each account identifies the access right rather than the real visitor. That allows multiple visitors share the same account of different level. An option to access DI/DO is provided for each account. Some users may need to prohibit from controlling your attached devices. You may delete some users from ③.

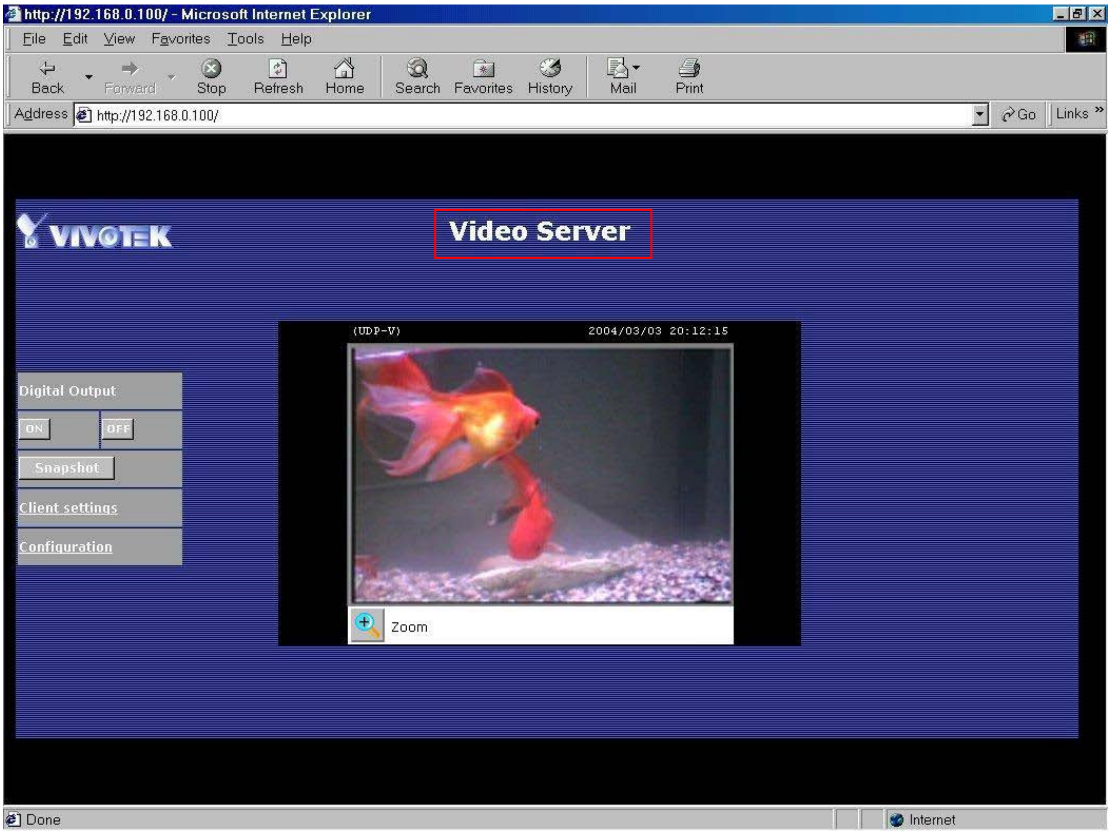
More flexible options for viewers ④

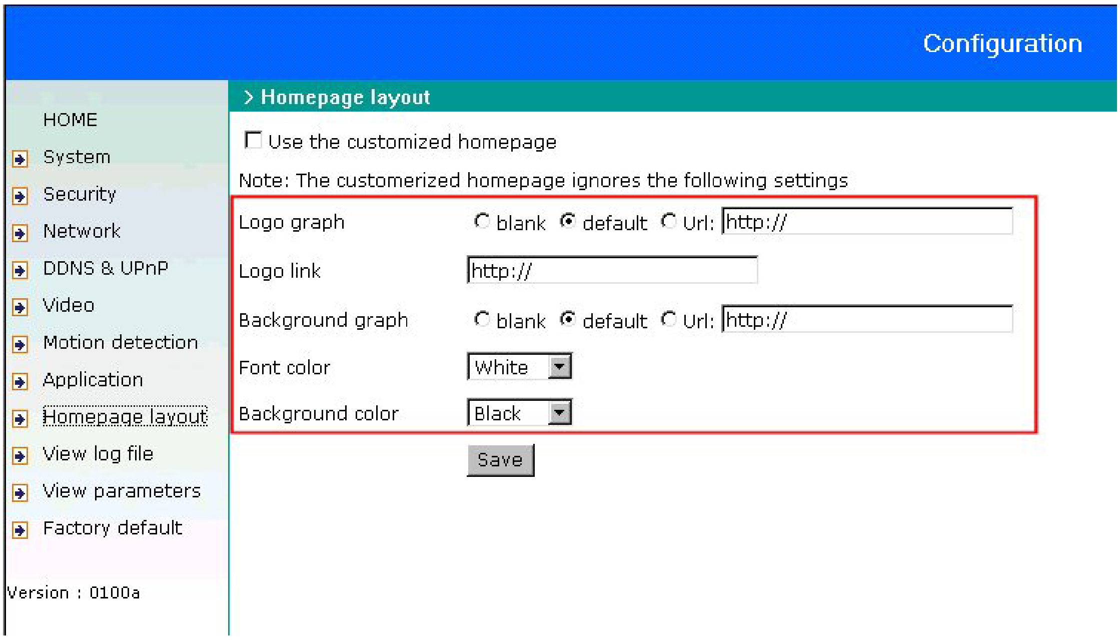
The first option allows anyone uses “demo” as the user name to view without password. The Administrator can also decide if more viewers are allowed to watch the video if the viewers exceed the limit. The overloaded viewers will have snapshot mode instead.

Change homepage layout

How to change the subject text of homepage

1. Click on “Configuration” on homepage,
2. Change the text in “Host name”,
3. Click on “Save” button.


http://192.168.0.100/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.0.100/
Go Links
VIVOTEK
Video Server
(UDP-V) 2004/03/03 20:12:15
Digital Output
ON OFF
Snapshot
Client settings
Configuration
Zoom
Done
Internet



> Homepage layout

□ Use the customized homepage

Note: The customerized homepage ignores the following settings

Logo graph	○ blank ● default ○ Url: http://
Logo link	http://
Background graph	○ blank ● default ○ Url: http://
Font color	White
Background color	Black

How to change the font color

1. Click on "Configuration" on homepage,

2. Click on "Homepage layout" at the left column,

3. Find "Font color" and pull down the list to choose any color you like,

4. Click on "Save" button.

* The font color is better to contrast with the background.

How to change the background

1. Click on "Configuration" on homepage,

2. Click on "Homepage layout" at the left column,

If you want to display simple color without any image,

3. Find "Background graph" and choose "blank",

4. Find "Background color" and pull down the list to choose any color you like,

5. Click on "Save" button.

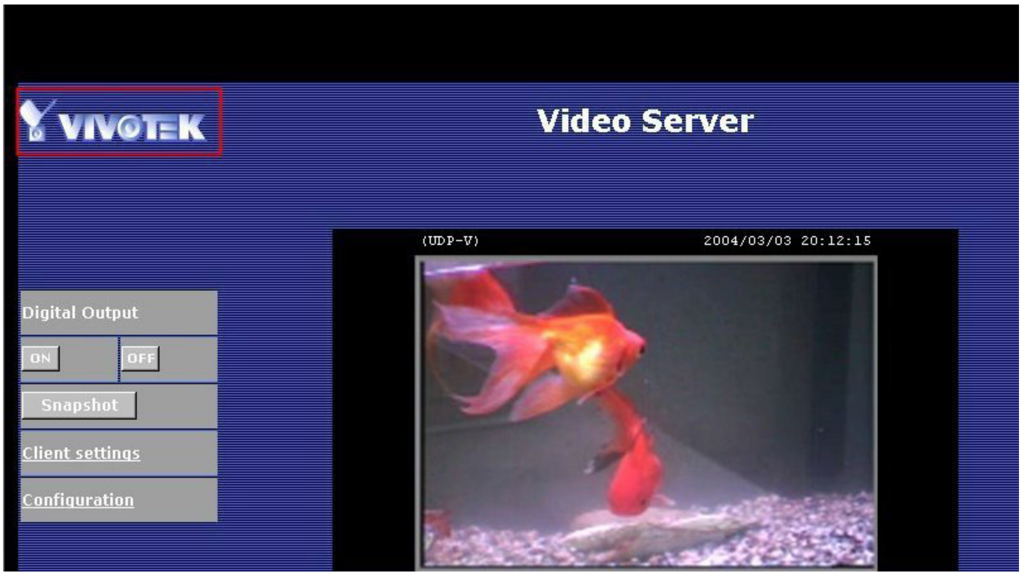
* The background color is better to contrast with the font.

If you want to use the image from another web site as background,

3. Find “Background graph” and choose “Url”,
4. Type the URL of the image on the Internet in the edit box, for example, “http://dgl.microsoft.com/thumbnails/j023/j0235217(t).gif”,
5. Click on “Save” button.

If you want to change the default background image stored in the Video Server,

3. Find “Background graph” and choose “default”,
4. Click on “Save” button,
5. Prepare an image file with size less than 131000 bytes and rename it to wallppr.jpg,
6. Open an FTP client program and connect to the Video Server. The user name and password is as same as the Administrator’s.
7. Transfer wallppr.jpg in local folder to the Video Server,
8. Close the FTP program and reload the homepage of the Video Server.



How to change the image logo at the upper left corner of homepage

1. Click on “Configuration” on homepage,
2. Click on “Homepage layout” at the left column,

If you want to remove any logo,

3. Find “Logo graph” and choose “blank”,
4. Click on “Save” button.

If you want to use the image from another web site as logo,

3. Find “Logo graph” and choose “Url”,
4. Type the URL of the image on the Internet in the edit box, for example, “http://dgl.microsoft.com/thumbnails/j023/j0234430(t).gif”,
5. Click on “Save” button.

If you want to change the default logo stored in the Video Server,

3. Find “Logo graph” and choose “default”,
4. Click on “Save” button,
5. Prepare an image file with size less than 65000 bytes and rename it to logo.gif,
6. Open an FTP client program and connect to the Video Server. The user name and password is as same as the Administrator’s.

7. Transfer logo.gif in local folder to the Video Server,
8. Close the FTP program and reload the homepage of the Video Server.

If you want to add hyperlink to the logo image,
3. Find “Logo link” and type the hyperlink in the edit box, for example, http://www.mywebsite.com,
4. Click on “Save” button.

How to design my own homepage to replace the current one

1. Prepare your own homepage with size less than 65000 bytes and rename it to user.htm,

2. Insert the html codes of video object, the bold Italian text in the following example, into the appropriate position in user.htm. Note that the codes of video object must be copied exactly the same including the letter case.

```
****** Example homepage begin ******
<html>
<head>
<title>Example – custom homepage</title>
</head>
<body background="/pic/wallppr.jpg">
<p>
   <a href="/setup/config.html">
   <img src="http://dgl.microsoft.com/thumbnails/j023/j0234430(t).gif"
align="left" width="64" height="64">
   </a>
   <font size="7" face="Comic Sans MS" color="#FF0000">
Video Server Demo
</font>
</p>
<p align="left">
<!-- Copy the next bold line to where you want to show the image coming from
Video Server. This line is remark only and is hidden on homepage. //-->
<OBJECT ID=VAMCtrl></OBJECT>
</p>
</body>
</html>
****** Example homepage end ******
```

3. Open an FTP client program and connect to the Video Server. The user name and password is as same as the Administrator’s.
4. Transfer user.htm in local folder to the Video Server,
5. Close the FTP program and reload the homepage of the Video Server,
6. Click on “Configuration” on homepage,
7. Click on “Homepage layout” at the left column,
8. Check “Use the customized homepage”.
9. Click on “Save” button and return to homepage.

* The user.htm only provides plain text content that scripts and URL of external resources can be used to adorn the homepage. Refer to tutorials of writing HTML and scripts.

⚠ If the customized homepage goes wrong and cannot display, link to the “Homepage layout” page, “http://<IP address of Video Server>/setup/layout.html”, to disable “Use the customized homepage”.

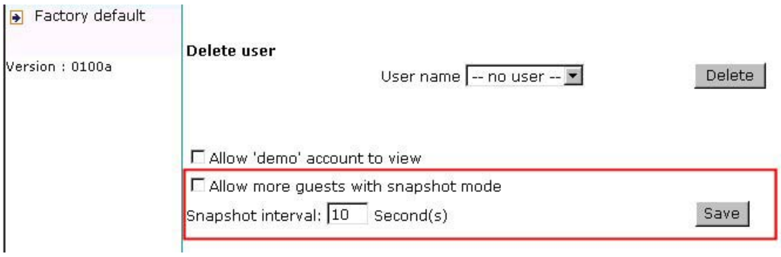
Build a multimedia web attraction site

Demo on multiple sites – mid-scale service

The Video Server can allow ten visitors on-line simultaneously. After Installation, focus the Video Server on any view you would like friends to share and tell the visitors to type in the web browser address. Caution: You may want to maintain your visitor's list in the security configuration page to block out unexpected visitors. No need to have the geeks' skill and equipments, no need to find suitable software.

Product demo for e-business – large-scale service

If the number of visitors has exceeded the limit, the Video Server can allow the "overload" viewers to see the snapshots in JPEG mode, on the homepage. These are still images and will be refreshed periodically and automatically. It needs a script function supported by the web browser.



Factory default

Version : 0100a

Delete user

User name: -- no user --

□ Allow 'demo' account to view

□ Allow more guests with snapshot mode

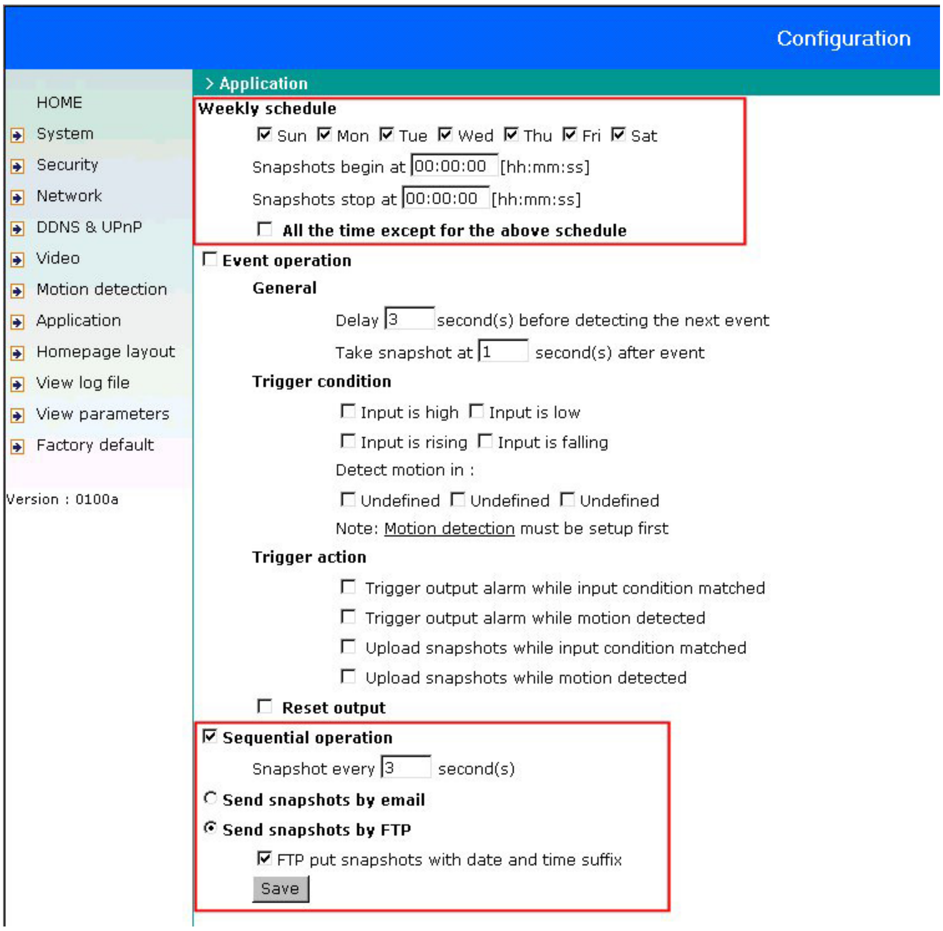
Snapshot interval: 10 Second(s)

1. Click on "Configuration" on homepage,
2. Click on "Security" at the left column,
3. Go to the page bottom and check "Allow more viewers with snapshot mode",
4. Set the snapshot interval to refresh the still image automatically. The longer the snapshot interval is, the better the snapshot mode works for more viewers.

If you want to expand to allow in more viewers, the host server should be able to handle large network traffic, which must handle the picture refreshing from the Video Server.

If the web space has FTP service,
Set the Video Server as an FTP client to upload the pictures. The access to the Video Server will be independent of the number of viewers and the picture quality will remain constant.

1. Click on “Configuration” on homepage,
2. Click on “Network” at the left column,
3. Fill the FTP related settings including server, user name and password, as well as the upload path if specified by the web space,
4. Click on save and wait for system restart,



Weekly schedule
☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat
Snapshots begin at 00:00:00 [hh:mm:ss]
Snapshots stop at 00:00:00 [hh:mm:ss]
□ **All the time except for the above schedule**

□ **Event operation**
General
Delay 3 second(s) before detecting the next event
Take snapshot at 1 second(s) after event
Trigger condition
□ Input is high □ Input is low
□ Input is rising □ Input is falling
Detect motion in :
□ Undefined □ Undefined □ Undefined
Note: Motion detection must be setup first
Trigger action
□ Trigger output alarm while input condition matched
□ Trigger output alarm while motion detected
□ Upload snapshots while input condition matched
□ Upload snapshots while motion detected
□ **Reset output**

☑ **Sequential operation**
Snapshot every 3 second(s)
○ **Send snapshots by email**
● **Send snapshots by FTP**
☑ FTP put snapshots with date and time suffix

5. Click on “Application” at the left column,

6. Select the weekday and daily schedule you want to upload the pictures,

7. Select “Sequential operation” and set the interval,

8. Select FTP without date time suffix as the upload method and click on save,

9. The image file uploaded to the web space is named “video.jpg”. Check if the file is successfully uploaded to the correct folder,

10. Prepare a homepage with the embedded image reference to the image file uploaded via FTP in advance.

If the web space has no FTP service,

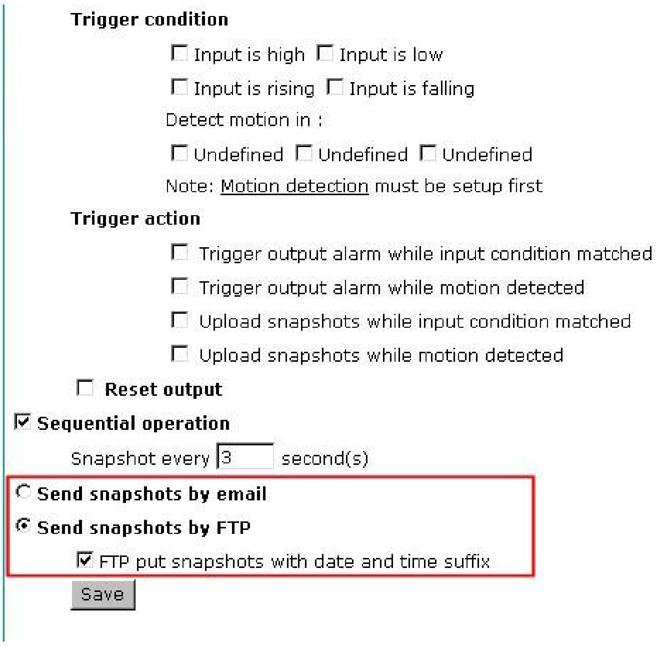
An auto-refresh homepage can be used to periodically poll the newest image from the Video Server. It is most efficient if using a free web space provider as the FTP service may be limiting.

1. Prepare an auto-refresh homepage like the following example. The URL of image is http://“IP address of the Video Server”/cgi-bin/video.jpg. Modify the IP address according to your Video Server. Define the refresh interval according to your network bandwidth for best result. If the refresh rate is too fast and there is a large number of visitors, this may overload the Video Server and slows the response.

```
****** Example homepage begin ******
<html>
<head>
<title>Example - auto refresh</title>
</head>
<body background="/pic/wallppr.jpg">
<p align=left>
  <font size="7" face="Comic Sans MS" color="#FF0000">
  Video Server Demo
  </font>
</p>
<p align=left>
<!-- Begin of scripts to auto refresh the image. Change the IP address in the image
URL and refreshrate if necessary. //-->
<script language=javascript>
var image="http://192.168.0.203/cgi-bin/video.jpg";          //IMAGE URL
var refreshrate=5;                    //SECONDS BETWEEN REFRESH
var imgwidth=352;                     //IMAGE WIDTH
var imgheight=240;                    //IMAGE HEIGHT (NTSC:240; PAL:288)
function refresh(){
document.images["pic"].src=image+"?"+new Date();
setTimeout('refresh()', refreshrate*1000);}
document.write('<img          src="'+image+'"          height="'+imgheight+'"
width="'+imgwidth+'" name="pic">');
if(document.images)window.onload=refresh;
</script>
<!-- End of scripts to auto refresh the image. //-->
</p>
</body>
</html>****** Example homepage end ******
```

Build a security application

The Administrator can combine options on the application page to perform many useful security applications. There are two trigger sources coming from attached devices such as for motion detection. There are also two kinds of actions responding to such events, including uploading snapshots over the Internet and driving other attached devices. To upload the snapshots, users can choose either email or FTP according to user's needs. Both e-mail and FTP use the network settings on the network page. Refer to the definition section for detail configuration.



Trigger condition

□ Input is high □ Input is low

□ Input is rising □ Input is falling

Detect motion in :

□ Undefined □ Undefined □ Undefined

Note: Motion detection must be setup first

Trigger action

□ Trigger output alarm while input condition matched

□ Trigger output alarm while motion detected

□ Upload snapshots while input condition matched

□ Upload snapshots while motion detected

□ **Reset output**

☑ **Sequential operation**

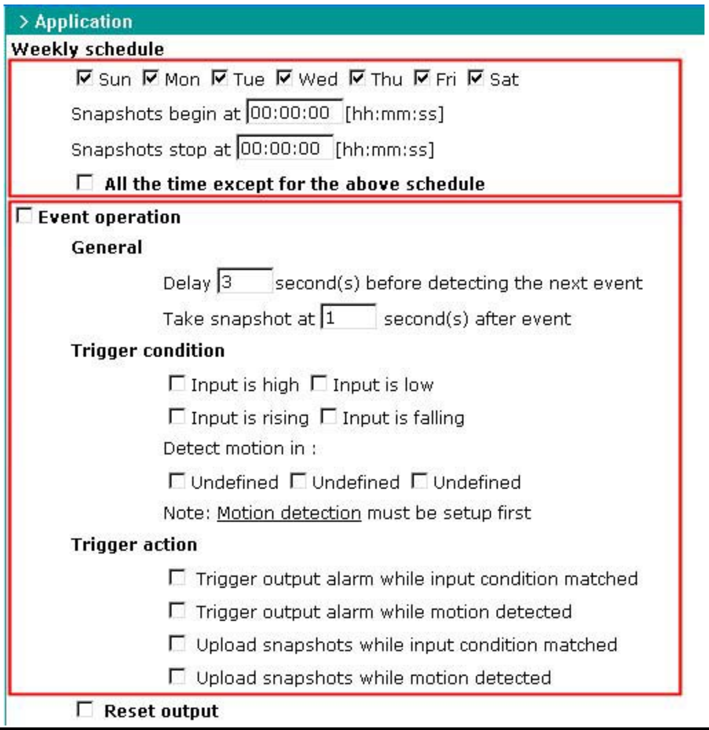
Snapshot every 3 second(s)

○ **Send snapshots by email**

● **Send snapshots by FTP**

☑ FTP put snapshots with date and time suffix

1. Click on "Configuration" on homepage,
2. Click on "Application" at the left column,
3. Check the weekdays as you need and give the period of "**Snapshots begin**" time and "**Snapshots end**" time to monitor the trigger conditions every day,
4. Check the "**Event operation**". The trigger condition can be set to detected motion or status of the attached device,



Weekly schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Snapshots begin at 00:00:00 [hh:mm:ss]

Snapshots stop at 00:00:00 [hh:mm:ss]

□ **All the time except for the above schedule**

□ **Event operation**

General

Delay 3 second(s) before detecting the next event

Take snapshot at 1 second(s) after event

Trigger condition

□ Input is high □ Input is low

□ Input is rising □ Input is falling

Detect motion in :

□ Undefined □ Undefined □ Undefined

Note: Motion detection must be setup first

Trigger action

□ Trigger output alarm while input condition matched

□ Trigger output alarm while motion detected

□ Upload snapshots while input condition matched

□ Upload snapshots while motion detected

□ **Reset output**

5. Set the delay **before detecting next event** to avoid continuous false alarms following the original event,

6. Set the delay to **take snapshots after event** to capture the direction of the moving objects,

Send snapshots when motion is detected

If no external sensor is available, Administrator can use the built-in motion detection to monitor any movement and send snapshots via email for security check.

7. Click on "**Motion detection**" at the left column,

8. Check "Enable motion detection",

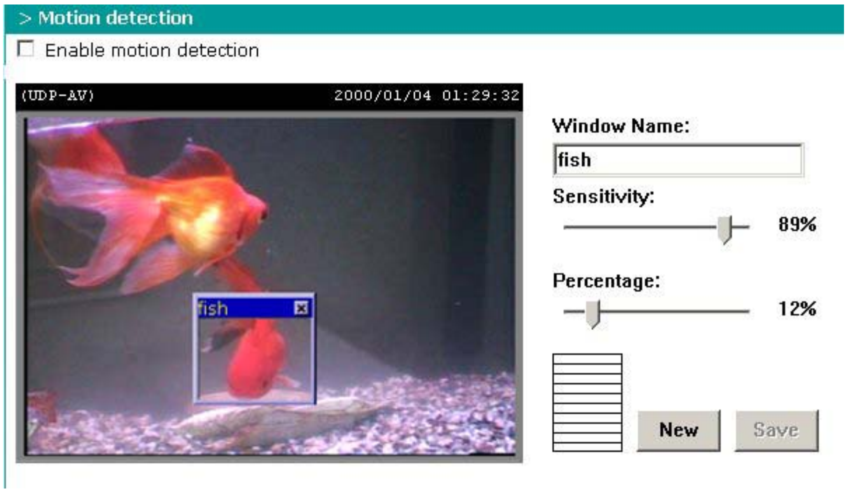
9. Click on new to have a new window to monitor video,

10. Type in a name to identify the new window,

11. Use the mouse to click, hold, and drag the window corner to resize or the title bar to move,

12. Fine-tune using the "Sensitivity" and "Percentage" fields to best suit the camera's environment. Higher "Sensitivity" detects the slighter motion. Higher "Percentage" discriminates smaller objects,

13. Clicking on "Save" enables the activity display. Green means the motion in the window is under the watermark set by Administrator and red means it is over the watermark,



> Motion detection

□ Enable motion detection

(UDP-AV) 2000/01/04 01:29:32

Window Name: fish

Sensitivity: 89%

Percentage: 12%

14. Click on "**Application**" at the left column,

15. Check the window name set in step 10,

16. Check “Upload snapshots while motion detected”, if e-mailing the snapshots is preferred,

17. Check “Send snapshots by email”,

18. Click on save to validate.

Software revision upgrade

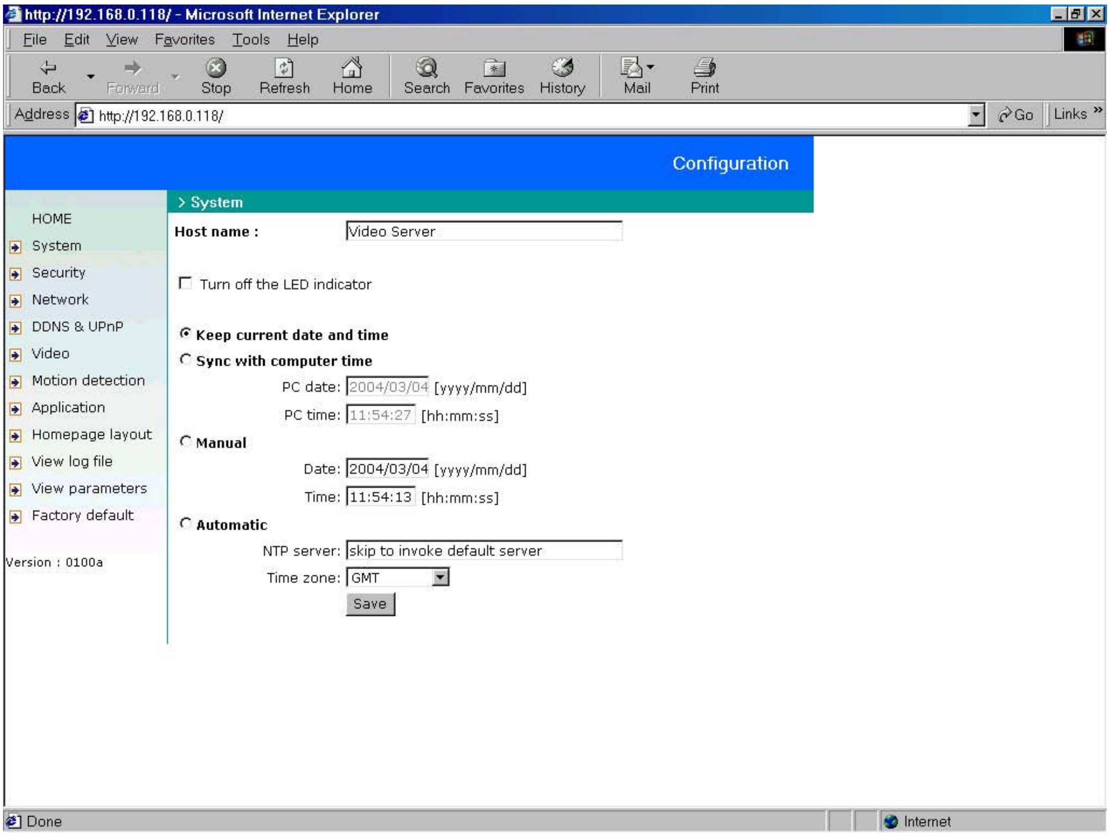
Customers can obtain the up-to-date software from the web site of Vivotek. An easy-to-use Installation Wizard is provided to upgrade the Video Server with just a few clicks. The upgrade function is opened to the Administrator only. To upgrade the system, follow the procedures below.

1. Download the firmware file named “FLASH.BIN” from the appropriate product folder.
2. Run the Installation Wizard and proceed following the prompts. Refer to the instructions of the Installation Wizard for details.
3. The whole process will finish in a few minutes and it will automatically restart the system.

⚠ If power fails during the writing process of Flash memory, the program in the memory of the Video Server may be destroyed permanently. If the Video Server cannot restart properly, ask your dealer for technical service.

Definitions in Configuration

Only the Administrator can access system configuration. Each category in the left column will be explained in the following pages. The bold texts are the specific phrases on the Option pages. The Administrator may type the URL below the figure to directly enter the frame page of configuration. If the Administrator also wants to set certain options through the URL, read the reference appendix for details.


http://192.168.0.118/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address http://192.168.0.118/
Go Links
Configuration
HOME
System
Security
Network
DDNS & UPnP
Video
Motion detection
Application
Homepage layout
View log file
View parameters
Factory default
Done
Internet

Version : 0100a

> System

Host name : Video Server

☐ Turn off the LED indicator

● **Keep current date and time**

○ **Sync with computer time**

PC date: 2004/03/04 [yyyy/mm/dd]

PC time: 11:54:27 [hh:mm:ss]

○ **Manual**

Date: 2004/03/04 [yyyy/mm/dd]

Time: 11:54:13 [hh:mm:ss]

○ **Automatic**

NTP server: skip to invoke default server

Time zone: GMT

Save

<url> *http://<Video Server>/setup/config.html*

<Video Server> is the domain name or original IP address of the Video Server.

System parameters

"Host name" The text displays the title at the top of the main page.
“Turn off the LED indicator” Check this option to shut off the LED beside the lens. It can prevent others from observing the operation.
"Keep current date and time" Click on this to reserve the current date and time of the Video Server. An internal real-time clock maintains the date and time even when the power of the system is turned off.
"Sync with computer time" Synchronizes the date and time of the Video Server with the local computer. The read-only date and time of the PC is displayed as updated.
“Manual” Adjust the date and time according to what is entered by the Administrator. Notice the format in the related fields while doing the entry.
“Automatic” Synchronize with the NTP server over the Internet whenever the Video Server starts up. It will fail if the assigned time-server cannot be reached.
“NTP server” Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Video Server to the default time-servers.
"Time zone" Adjust the time with that of the time-servers for local settings.

Remember to click on Save to immediately validate the changes. Otherwise, the correct time will not be synchronized.

Security settings

"Root password" Change the Administrator's password by typing in the new password identically in both text boxes. The typed entries will be displayed as asterisks for security purposes. After pressing Save, the web browser will ask the Administrator for the new password for access.

"Add user" Type the new user's name and password and press Add to insert the new entry. The new user will be displayed in the user name list. There is a maximum of twenty user accounts. Each user can have the privilege to "**Permit for I/O control**".

"Delete user" Pull down the user list to find the user's name and press Delete to complete.

"Allow 'demo' account to view" Click this to permit anyone who types in "demo" as user name. No password is needed for demo account. Note that a demo account is restricted to view only.

"Allow more viewers with snapshot mode" There can only be a maximum of 10 users to simultaneously view the video. This option allows for the 11th viewer on, the overloaded viewers, to see only still images. These still images are automatically refreshed by the interval defined below. This feature must be supported by the java script capability of the web browsers.

"Snapshot interval" defines the refresh rate of the still image in the homepage seen by the overloaded viewers.

Network settings

Any changes made on this page will restart the system in order to validate the changes. Make sure every field is entered correctly before clicking on Save.

"Reset IP address at next boot", the default status is checked to get IP address automatically at the server start. Therefore, once the network settings, especially the IP address, have been entered correctly, uncheck this option.

General

"IP address" This is necessary for network identification.

"Subnet mask" This is used to determine if the destination is in the same subnet. The default value is "255.255.255.0".

"Default router" This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will fail the transmission to destinations in different subnet.

"Primary DNS" The primary domain name server that translates hostnames into IP addresses.

"Secondary DNS" Secondary domain name server that backups the Primary DNS.

SMTP

When the SMTP server support SMTP authentication, users need to give the valid user name and password to send email via the server.

"SMTP (mail) server 1" The domain name or IP address of the external email server.

"User name of SMTP 1" This granted user name on the external email server.

"Password of SMTP 1" This granted password on the external email server.

"Recipient email address 1" The email address of the recipients for snapshots or log file. Multiple recipients must be separated by semicolon, ';'.

"SMTP (mail) server 2" The domain name or IP address of another email server once the previous server is unreachable.

"User name of SMTP 2", granted user name on the backup email server.
"Password of SMTP 2", granted password on the backup email server.
"Recipient email address 2" The email address of the recipients for the backup server.
"Sender email address", the email address of the sender.

FTP

"Local FTP server port" This can be other than the default port 21. The user can change this value from 1 to 65535. After the changed, the external FTP client program must change the server port of connection accordingly.
"1st FTP server" The domain name or the IP address of the external FTP server. The following user settings must be correctly configured for remote access.
"1st FTP user name" Granted user name on the external FTP server.
"1st FTP password" Granted password on the external FTP server.
"1st FTP remote folder" Granted folder on the external FTP server. The string must conform to that of the external FTP server. Some FTP servers cannot accept preceding slash symbol before the path without virtual path mapping. Refer to the instructions for the external FTP server for details. The folder privilege must be open for upload.
"Primary FTP passive mode" The Video Server is located inside the network protected by a firewall, data connection for FTP may be prohibited. By selecting passive mode, the FTP can bypass the rule and allow snapshot upload to proceed. If the passive mode is selected, the Video Server can automatically attempt for active mode, if the external FTP server does not support passive mode.
"2nd FTP server" The domain name or IP address of the external FTP server.
"2nd FTP user name" Granted user name on the backup FTP server.
"2nd FTP password" Granted password on the backup FTP server.
"2nd FTP remote folder" Granted folder on the backup FTP server.
"Secondary FTP passive mode" Passive mode setting for the backup FTP server.

HTTP

"Http port" This can be other than the default Port 80. Once the port is changed, the users must be notified the change for the connection to be successful. For instance, when the Administrator changes the HTTP port of the Video Server whose IP address is 192.168.0.100 from 80 to 8080, the users must type in the web browser "http://192.168.0.100:8080" instead of "http://192.168.0.100".

Streaming

"Control channel port" This can be something other than the default port 5001 in order to work with the port opened by the firewall.
"Audio channel port" This can be something other than the default port 5002 in order to work with the port opened by the firewall.
"Video channel port" This can be something other than the default port 5003 in order to work with the port opened by the firewall.
"Improve audio quality in low bandwidth environment" If the Video Server seems to work in a low bandwidth network environment, the user can use this option to see if audio quality can be improved by sacrificing some real-time synchronization.
"Mute" This can force the transmission protocol to HTTP and disable audio.

⚠ Some invalid settings may cause the system failing to respond. Change the configuration only if necessary and consult with your network supervisor or experienced users for correct settings. Once the system has lost contact, refer to Appendix A for reset and restore procedures.

DDNS and UPnP settings

"Enable DDNS" This option turns on the DDNS function.
"Provider" The provider list contains four hosts that provide DDNS services. Please connect to the service provider's website to make sure the service charges.
"Host name" If users wants to use DDNS service, this field must be filled. Please input the hostname that is registered in the DDNS server.
"Username/E-mail" The Username or E-mail field is necessary for logging in the DDNS server or notify users of the new IP address. **Note**: when this field is input as **"Username"** the following field must be input as **"Password"**.
"Password/Key" Please input the password or key to get the DDNS service.
"**Enable UPnP presentation**" This turns on or off the UPnP function. When UPnP is turned off, the camera cannot be found through network neighbors in MS Windows XP. If the UPnP network component is installed in Windows XP, the hostname of the Video Server will be shown with bracketed IP address in the Network neighbors. Ex: Video Server (192.168.0.96). That is: The hostname of the Video Server is "*Video Server*"*,* and the IP address of the Video Server is *192.168.0.96.*
"**Enable UPnP port forwarding**" If the network router supports port forwarding function, the Administrator can check the option to enable this function. The Network Camera will negotiate the ports provided by the router after rebooted. During the negotiation, the control channel port, video channel port and audio channel port are configured automatically. One exception is if the http port number conflicts the port number owned by other network devices, the Network Camera will have a warning message on the network settings page. The HTTP port number is assigned manually, for that users might not access the web pages if HTTP port number is unknown. Users can access the Network Camera through Internet using different port provided by the router, after the four ports are configured correctly.**" Save"** Click on the button to save current settings for the DDNS service and UPnP function.
Network Camera provides a free DDNS service. Administrators can choose safe100.net in the "Providers" field to use it. At the first time, Administrators must register an account for it.

Video codec parameters

"Text on video" The text will be displayed in the black bar above the video window with a timestamp. The timestamp is captured from the date and time of the Video Server that is maintained by a built-in real-time clock.

"Color" Select either for color or monochrome video display.

"Size" There are five options for three video sizes. **"Half"** is the quarter size of **"Normal"**. **"Half x 2"** has the same video size as **"Normal"** but of a lesser quality, while consuming less network bandwidth. **"Normal"** is the quarter size of **"Double"**. **"Normal x 2"** has the same video size as **"Double"** but of a lesser quality, while consuming less network bandwidth.

"Modulation" The type of video modulation depended on the type of camera. The type is auto-detected during initialization, but the Administrator can still set it manually.

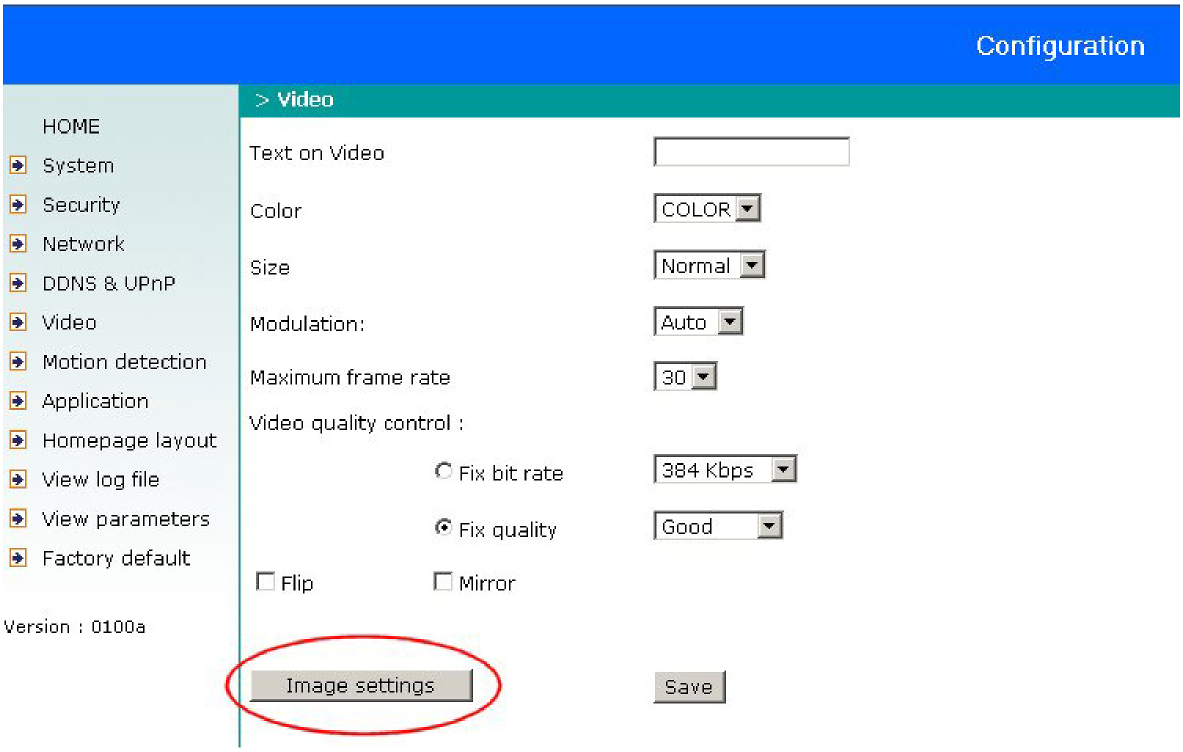
There are three dependent parameters provided for video performance adjustment.

"Maximum frame rate" This limits the maximal refresh frame rate, which can be combined with the **"Video quality control"** to optimize bandwidth utilization and video quality. If the user wants to fix the bandwidth utilization regardless of the video quality, choose **"Fix bit rate"** and select the desired bandwidth. The video quality may be poor due to the sending of maximal frame rate within the limited bandwidth when images are moving rapidly. Consequently, to ensure detailed video quality (quantization rate) regardless of the network, it will utilize more bandwidth to send the maximal frames when images change drastically.

"Flip" Vertically rotate the video.

"Mirror" Horizontally rotate the video. Check options both if the Video Server is installed upside down.

Image settings Click on this button to pop up another window to tune **"Brightness"**, **"Contrast"**, **"Hue"** and **"Saturation"** for video compensation. Each field has eleven levels ranged from -5 to +5. The user may press Preview to fine-tune the image. When the image is O.K., press Save to set the image settings. Restore Click on this to recall the original settings without incorporating the changes.



> Video

Text on Video

Color: COLOR

Size: Normal

Modulation: Auto

Maximum frame rate: 30

Video quality control :

○ Fix bit rate: 384 Kbps

● Fix quality: Good

□ Flip □ Mirror

Motion detection

"Enable motion detection" Check this option to turn on motion detection.

New Click on this button to add a new window. At most three windows can exist simultaneously. Use the mouse to click, hold, and drag the window frame to resize or the title bar to move. Clicking on the 'x' at the upper right-hand corner of the window to delete the window. Remember to save in order to validate the changes.

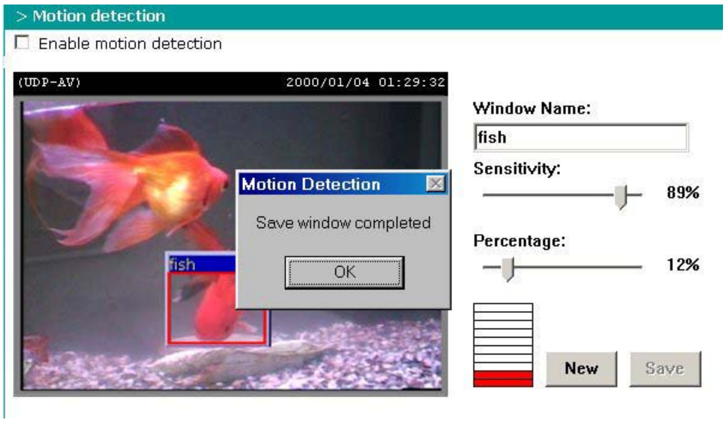
Save Click on this button to save the related window settings. A graphic bar will rise or fall depending on the image variation. A green bar means the image variation is under monitoring level and a red bar means the image variation is over monitoring level. When the bar goes red, the detected window will also be outlined in red. Going back to the homepage, the monitored window is hidden but the red frame shows when motion is detected.

"Window Name" The text will show at the top of the window.

"Sensitivity" This sets the endurable difference between two sequential images.

"Percentage" This sets the space ratio of moving objects in the monitoring window. Higher sensitivity and small percentage will allow easier motion detection.

The following figure shows the screen when Save is clicked. The monitoring window has been outlined in red and the graphic bar goes red since the goldfish is moving.



> Motion detection

□ Enable motion detection

(UDP-AV) 2000/01/04 01:29:32

Motion Detection

Save window completed

Window Name: fish

Sensitivity: 89%

Percentage: 12%

Application settings

Weekly schedule

"Sun" ~ "Sat" Select the days of the week to perform the following operations.
"Snapshots begin at" Set the time to start operations.
"Snapshots stop at" Set the time to stop operations.
Setting identical begin time and stop time means 24-hour operation.
"All the time except for the above schedule" Set the schedule all the time except for the above in a week.

Event operation

"Delay second(s) before detecting next event" Set the time delay before restarting to check on the triggering condition when the current condition is triggered.
"Take snapshots at second(s) after event" After the camera has taken a snapshot when a condition is triggered, another snapshot will be taken after this configured interval, in seconds.
"Trigger condition" There are four conditions relative to the digital input and the three windows for motion detection. More than one condition can be selected at once. Select the appropriate digital input condition that suits the characteristics of the external device. "high", "low" selects level-triggering via external voltage input. "rising", "falling" is for edge-triggering. There are three windows for motion detection each can be assigned a name. If motion detection has not been set up, "**undefined**" will be shown instead of the window title. If this happens, clicking on "Motion detection" and a note will show to direct the User to the configuration page for motion detection.
"Trigger action" There are four options for two types of action. More than one condition can be selected at once. While choosing to trigger an output alarm, the digital output will short both pins and complete the external device's circuit. The normal state is open. Either email or FTP can be used to command uploading snapshots. The snapshot names will be "vpre.jpg", "vtrg.jpg", and "vpos.jpg", respectively. They stand

for the snapshots, before event, right upon event, and after event. The date and time suffix may also be added as an option. Confirm the external mail or FTP server settings in the network configuration.

“**Reset output**” Select and save this option to reset the external device at the digital output to return to the original state.

Sequential operation

“Snapshot every second(s)” The Video Server will send snapshots at the specified intervals to the external server using the method selected below. Remember: This operation is still subject to the conditions set in the weekly schedule.

“Send snapshots by email” This selects the uploading method following the intervals set above. The snapshot named “video.jpg” will be attached in the email with the subject title “Periodic snapshots”.

“Send snapshots by FTP” The snapshots will be uploaded to the external FTP server with the file name defined in the next option. This can also be used to refresh the captured images stored in the external web server to build creative homepages.

“FTP put snapshots with date and time suffix” This option sets up the snapshot capture date and time, which can be used to easily differentiate the snapshot file names in either the sequential or event operation. For instance, “video@20030102030405.jpg” means the JPEG image was captured in the year 2003, January the 2nd, at 3 o’clock, 4 minute, and 5 second. If this suffix is omitted, the file named “video.jpg” on the external FTP server will be refreshed at the specified interval.

Homepage layout settings

"Use the customized homepage", check this option to use "user.htm" uploaded by the Administrator instead of the default one. Refer to the section "Administrator's capability" for detail usage. The following options related to the default homepage will not affect the "user.htm".

"Logo graph", the logo located at the upper left corner of homepage can be hidden, the default one that can be changed by the Administrator, or any image on the Internet that can be located via URL. The default logo is stored in memory and can be changed by FTP. The maximal size is 32000 bytes. Though the file name is fixed to "logo.gif", the image can be any file format as long as the web browser can read it. Refer to the section "Administrator's capability" for how to change the default logo.

"Logo link", when users click on the logo image, a new window will pop up to show the homepage of the given URL. Clear the URL will disable the link function.

"Background graph", the background image can be hidden to show the background color only, the default one that can be changed by the Administrator, or any image on the Internet that can be located via URL. The default background image is stored in memory and can be changed by FTP. The maximal size is 131000 bytes. Though the file name is fixed to "wallppr.jpg", it can be any file format as long as the web browser can read it. Refer to the section "Administrator's capability" for how to change the background image.

"Font color", pull down the list to select any color for the text in the homepage.

"Background color", pull down the list to select any color for the homepage background. It can be seen when the background image is not displayed.

Viewing system log

Click the link on the configuration page to view the system log file. The content of the file provides useful information about configuration and connection after system boot-up.

Viewing system parameters

Click on this link on the configuration page to view the entire system's parameter set. The content is the same as those in CONFIG.INI.

Factory default

Click on this link on the configuration page to restore the factory default settings. Any changes made so far will be lost and the system will be reset to the initial factory settings. After clicking on the "Restore" button and make confirmation, the system will restart and require the installer program to set up the network again.

Appendix

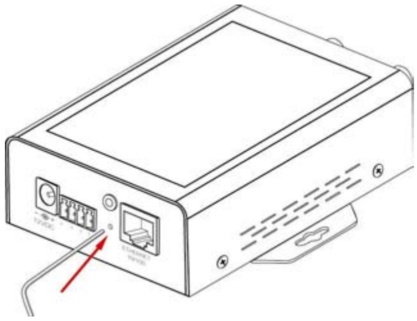
A. Troubleshooting

Status LED

After powering up, the Video Server performs a self-diagnostic to detect any hardware defects. The following table lists the LED patterns in general. In case of any fatal error, the LED will blink in a pattern other than those below.

Condition	LED color
During self-diagnostic after power on	Blink in interchanged green and red
Ethernet signal is lost	Steady red till Ethernet is detected
Before network is setup	Steady green till IP address is confirmed
After network is setup	Blink green every second
Any hardware failure	Other patterns

Reset and restore



⚠ Restoring the factory defaults will erase any previous settings. Reset or restore the system after power on.

There is a button hidden in the pinhole beside the Ethernet socket. It is used to reset the system or restore the factory default settings. Sometimes resetting the system sets the system back to normal state. If the system problems remain after reset, restore the factory settings and install again.

RESET: Poke the wrench to click on the button.

RESTORE: 1. Poke the wrench to press on the button continuously.

2. Wait for self-diagnostic to run twice.

3. Withdraw the wrench as soon as the second self-diagnostic starts.

B. Frequently asked questions

Q What if I forget my password?

A After the Administrator's password is assigned, every access to the Video Server needs authentication. If you are one of the managed users, you have to ask the Administrator for the password. If you are the Administrator, there is no way to recover the root password except for restoring factory default. Refer to Appendix A for the procedures.

Q Why can I not watch video from the Video Server after it is authenticated?

A There are many possible scenarios regarding this problem,

1. If you have just installed the Video Server and are unable to watch the video, check if the heartbeat LED is blinking or the lens cap is removed. If the heartbeat LED is dim, perform the software installation again.
2. If the Video Server is well installed and you are accessing the Video Server for the first time using Internet Explorer, adjust the security level of Internet Explorer to allow installation of plug-ins.
3. If the problem still exists after adjusting, and the message over the image window is showing "connecting", the network traffic may be too crowded.

Q What is the plug-in for?

A The plug-in provided by the Video Server is used to display motion pictures and audio in Internet Explorer. If your system does not allow installation of any plug-in software, the security level of the web browser may need to be lowered. It is recommended that you consult your network supervisors in your office regarding adjustment of the security level. Software installation may be regulated in some offices.

Q Why is the timestamp different from the system time of my PC or notebook?

A The timestamp is based on the system time of the Video Server. It is maintained by a real-time clock inside and can be automatically synchronized with the time server if the Video Server is connected to the Internet and the function is enabled. Differences of several hours may result from the time zone setting.

Q Can I install it on ceiling?

A Yes. There are flip and mirror options in video configuration page to correct the images for upside down installation.

Q The image is not clear enough.

A Rotate the lens to adjust the focus after the Video Server is installed in the proper position. The image settings and white balance can be fine tuned to achieve the best visual effect. Also notice the power line frequency must match the local utility to synchronize and minimize the effect of flickering florescent lights.

Q Why does the image not refresh regularly?

A Some anti-virus programs filter the received web content. It takes time to perform data examination and affect the streaming application such as the Video Server. However it only affects the HTP mode of the Video Server. If the network allows only HTTP mode, disable the web filtering function of the anti-virus program temporarily. During the period, users should be aware of the risk of malicious network activity.

Q I have opened motion detection windows but it cannot work.

A If the motion detection windows are setup and names are given, check to see if the function is checked at the first line. While it is enabled, adjust the sensitivity and percentage to monitor the level indicator for best results.

Q I cannot hear any sound while watching.

A If there is "V_ONLY" shown above the image, click on connection type to uncheck "Disable audio". If there is "V" shown instead of "AV", the sound card in your PC may not properly installed. If "AV" is shown, check the audio source of the Video Server.

Q How many users are allowed to watch the Video Server at the same time?

A Too many users requesting the real-time multimedia content will jam the network. For best results, the Video Server is designed to accommodate maximum ten (10) users to watch and listen to the Video Server at the same time. For a larger number of users, it is recommended to build another web server to host the retrieving contents from the Video Server.

Q How fast is the video rate of the Video Server?

A The MPEG4 codec engine can process 30 frames per second internally. However the total performance is subject to many coefficients as follows:

1. Network throughput,
2. Bandwidth share,
3. Number of users,
4. The complicated/detailed objects and movement in view,
5. The level of your PC or notebook computer that is responsible for displaying images.

In general, the transfer rate in a general local network environment can achieve over 200 kilobytes per second and approximately 10 to 20 pictures per second from a regular environment.

Q How can I keep the Video Server as private as possible?

A The Video Server is designed for surveillance purposes and has many flexible interfaces. The user authentication and special confirmation in installation can keep the Video Server from unauthorized access. You may also change the HTTP port to non-public number. The demo account is good to separate guests from normal users and thus you can easily block guests anytime. You can check the system log to examine any abnormal activities and trace the origins.

Q Why can I not access the Video Server when I setup some options in the application?

A Since the Video Server is a "network device", any incorrect network settings will make it unreachable. If this happens, restore the factory default settings following the procedures in Appendix A.

C. URL commands of the Video Server

For some customers who already have their own web site or web control application, the Video Server can be easily integrated through convenient URLs. This section lists the commands in URL format corresponding to the basic functions of the erase Video Server.

Capture update Snapshot of JPEG image

/cgi-bin/video.jpg
The Video Server will return the most up-to-date snapshot in JPEG format.

Query status of the digital input

/cgi-bin/getdi.cgi
The Video Server will return the status of digital input.

Drive the digital output

/cgi-bin/setdo.cgi?do=<state>
The state is either "H", or "L"."H" means high, that is NC is connected with COMMON and "L" means low that is NO is connected with COMMON.
For instance, typing http://192.168.0.201/cgi-bin/setdo.cgi?do=h in the address bar of the web browser will command the Video Server, with IP address of 192.168.0.201, to set digital output to connect to NC with COMMON.

Restore factory default settings

/setup/restore.cgi

The Video Server will automatically restart after restoring factory default configurations.

Restart system

/setup/reset.cgi
Restart the Video Server without warning.

Page URL

The configuration page has a frame layout including an option list frame and an option page frame. Referenced URLs, except for the configuration page, direct users to the option page frame only. Some pages, such as image quality setting and preset setting, are opened in new windows for preview.

Only the Administrator can access these URLs.

Homepage name	Referenced URL
connection type page	/client.html
configuration page	/setup/config.html
system option	/setup/system.html
security option	/setup/security.html
network option	/setup/network.html
video option	/setup/video.html
motion detection	/setup/motion.html
image quality option	/setup/image.html
application option	/setup/app.html
homepage layout option	/setup/layout.html
system log	/setup/logfile.html
system parameters	/setup/parafile.html
set factory default	/setup/factory.html

System resource URL

There are some images used on the homepage when the homepage layout is in image mode. The Administrator may use the following links to show the images saved in the Video Server on another page.

Resource name	Referenced URL
system logo image	/pic/logo.gif
background image	/pic/wallppr.jpg

General format of command URL

Every configuration can be set through URL with POST method by the Administrator only.

<general format>

URL[?[name=value][&name=value]......]

<method>

POST

<authorized user>

root

System configuration URL

URL: /setup/system.cgi

NAME	VALUE	DESCRIPTION
host	<text string shorter than 15 characters>	system name
Ledoff	yes	turn off front LED
	no	turn on front LED
method	keep	keep date and time unchanged
	auto	use NTP server to synchronize
	manu	directly adjust date and time
date	<yyyy/mm/dd>	year, month and date separated by slash
time	<hh:mm:ss>	hour, minute and second separated by colon
ntp	<domain name or IP address>	NTP server
zone	-12 ~ 12	time zone, 8 means GMT +8:00

Security configuration URL

URL: /setup/security.cgi

NAME	VALUE	DESCRIPTION
rootpass	<text string shorter than 15 characters>	change root password
username	<text string shorter than 15 characters>	add new user
userpass	<text string shorter than 15 characters>	new user's password
deluser	<text string shorter than 15 characters>	existing user name
action	<blank>	validate demo users with “open”
open	yes	grant for demo account
	no	prohibit for demo account
dido	yes	permission for DIDO access
	no	prohibit for DIDO access

Network configuration URL

URL: /setup/network.cgi

NAME	VALUE	DESCRIPTION
reset	yes	enable installation at next boot
	no	disable installation at next boot
ip	<IP address>	Video Server's IP address
subnet	<IP address>	subnet mask
router	<IP address>	default gateway
domain	<text string shorter than 40 characters>	domain name of Video Server
dns1	<IP address>	primary DNS server
dns2	<IP address>	secondary DNS server

smtp1	<domain name or IP address>	primary SMTP server
smtp1Usr	<string shorter than 39 characters>	user name for primary SMTP server
smtp1pass	<string shorter than 39 characters>	password for primary SMTP server
mail1	<string shorter than 80 characters>	mail recipient address
smtp2	<domain name or IP address>	secondary SMTP server
smtp2Usr	<string shorter than 39 characters>	user name for secondary SMTP server
smtp2pass	<string shorter than 39 characters>	password for secondary SMTP server
mail2	<text string shorter than 80 characters>	mail recipient address
returnemail	<text string shorter than 80 characters>	return email address
ftpp	<number less than 65535>	FTP port
ftp1	<domain name or IP address>	primary FTP server
ftpuser1	<text string shorter than 15 characters>	user name for primary FTP server
ftppass1	<text string shorter than 15 characters>	password for primary FTP server
ftpfolder1	<text string shorter than 40 characters>	upload folder in primary FTP server
Pasv1	yes	access FTP server in passive mode
	no	access FTP server in active mode
ftp2	<domain name or IP address>	secondary FTP server
ftpuser2	<text string shorter than 15 characters>	user name for secondary FTP server
ftppass2	<text string shorter than 15 characters>	password for secondary FTP server
ftpfolder2	<text string shorter than 40 characters>	upload folder in secondary FTP server

Pasv2	yes	access FTP server in passive mode
	no	access FTP server in active mode
http	<number less than 65535>	HTTP port
cport	<number less than 65535>	control Channel port
aport	<number less than 65535>	audio Channel port
vport	<number less than 65535>	video Channel port
band	yes	optimal for the low bandwidth
	no	keep the original way
mute	yes	disable audio
	no	enable audio

DDNS & UPnP configuration URL

URL: /setup/ddns.html

NAME	VALUE	DESCRIPTION
enddns	anything	Enable DDNS function. This option must be resent whenever the URL is called, if DDNS function is to be enabled.
provider	1	DynDNS.org(Dynamic)
	2	DynDNS.org(Custom)
	3	TZO.com
	4	dhs.org
host	<text string shorter than 40 characters>	The hostname of the Video Server
usermail	<text string shorter than 40 characters>	The login username of DDNS server or the email address registered in DDNS server.
passkey	<text string shorter than 40 characters>	The login password of DDNS server or the key given by the DDNS server.

enupnp	yes, no	Enable UPnP function. This option must be resent whenever the URL is called, if UPnP function is to be enabled.
enupnpnat	yes, no	Enable UPnP port forwarding.

Video configuration URL

URL: /setup/video.cgi

NAME	VALUE	DESCRIPTION
text	<text string shorter than 15 characters>	enclosed caption
color	B/W	monochrome
	<other than B/W>	color
size	1	half
	2	half x 2
	3	normal
	4	normal x 2
	5	double
mode	Auto	auto detect the camera type
	NTSC	set the camera type to NTSC
	PAL	set the camera type to PAL
quality	fixb	fix bit rate
	<other than fixb>	fix quantization
quan	1	lowest quality of video
	2	lower quality of video
	3	normal quality of video
	4	higher quality of video
	5	highest quality of video
bitrate	64000	set bit rate to 64K bps
	128000	set bit rate to 128K bps

	256000	set bit rate to 256K bps
	384000	set bit rate to 384K bps
	512000	set bit rate to 512K bps
	768000	set bit rate to 768K bps
	1000000	set bit rate to 1000K bps
	1200000	set bit rate to 1200K bps
frame	1	set maximum frame rate to 1 fps
	2	set maximum frame rate to 2 fps
	3	set maximum frame rate to 3 fps
	5	set maximum frame rate to 5 fps
	10	set maximum frame rate to 10 fps
	15	set maximum frame rate to 15 fps
	20	set maximum frame rate to 20 fps
	25	set maximum frame rate to 25 fps
	30	set maximum frame rate to 30 fps
flip	yes	flip image
	no	normal image
mirror	yes	mirror image
	no	normal image

Image quality configuration URL

URL: /setup/image.cgi

NAME	VALUE	DESCRIPTION
brightness	<-5 ~ 5>	adjust brightness of image
contrast	<-5 ~ 5>	adjust contrast of image
hue	<-5 ~ 5>	adjust hue of image
saturation	<-5 ~ 5>	adjust saturation of image
preview	<not required>	not save the parameters
restore	<not required>	recall the original settings
save	<not required>	save the parameters

Application configuration URL

URL: /setup/app.cgi

NAME	VALUE	DESCRIPTION
emode	<not required>	event mode application
smode	<not required>	sequential mode application
smethod	mail	upload snapshots by email
	ftp	upload snapshots by FTP
suffix	<not required>	FTP file with date and time suffix
delay	<integer>	seconds delay to detect next event
inter	<integer>	seconds delay to capture post-event
dihigh	< not required >	set DI high as trigger condition
dilow	< not required >	set DI low as trigger condition
dirise	< not required >	set DI rising as trigger condition
difall	< not required >	set DI falling as trigger condition
motion1	< not required >	set motion window1 as trigger condition
motion2	< not required >	set motion window2 as trigger condition
motion3	< not required >	set motion window3 as trigger condition
ioalarm	< not required >	trigger DO when DI condition matched
mdalarm	< not required >	trigger DO when motion detected
ioupload	< not required >	upload snapshot when DI condition matched
mdupload	< not required >	upload snapshot when motion detected
sinter	<integer>	seconds interval for sequential mode
sbegin	<hh:mm:ss>	time to start sequential mode
send	<hh:mm:ss>	time to stop sequential mode

Homepage layout configuration URL

URL: /setup/layout.cgi

NAME	VALUE	DESCRIPTION
cuslogo	blank	hide logo
	def	use default logo
	url	use image from URL
logourl	<text string shorter than 80 characters>	URL of image for logo
linkurl	<text string shorter than 80 characters>	URL to link when clicking on logo
cusback	blank	hide background image
	def	use default background
	url	use image from URL
backurl	<text string shorter than 80 characters>	URL of image for background
fcolor	<0 ~ 15>	color index for font
bcolor	<0 ~ 15>	color index for background

D. Technical specifications

- System

CPU: Trimedia PNX1300
RAM: 8MB SDRAM
ROM: 2MB FLASH ROM

- Networking

Protocol

TCP/IP, HTTP, SMTP, FTP, Telnet, NTP, DNS, DHCP, DRM, DDNS and UPnP

Physical

10BaseT Ethernet or 100BaseT Fast Ethernet

- Video

Algorithm supported

MPEG4(short header mode)

Video Input

1 BNC composite video input
NTSC/PAL auto-sensing

Video Output

1 BNC composite video output

Features

Adjustable image size, quality and bit rate
Timestamp and text overlay
3 motion detection windows

Resolution

NTSC

Up to 30 frames at 176x120
Up to 30 frames at 352x240
Up to 10 frames at 702x480

PAL

Up to 25 frames at 176x144
Up to 25 frames at 352x288
Up to 10 frames at 702x576

- Audio

Algorithm supported

24Kbps

Audio Inputs

1 RCA mono audio input

- General I/O

1 sensor input(max. 12VDC 50mA)
1 relay output(max. 24VDC 1A, 125VAC 0.5A)

- LED indicator

Dual color status indicator

- Dimension

116mm(L) * 80mm(W) * 35mm(H)

- Weight

NET. 339g

- Power

Consumption: near 5.4W
Universal switching power supply included
Input: 100-240VAC, 50/60Hz, 0.4A
Output: 12VDC, 1.5A

- Operating Environment

Temperature: 0-50°C/32-122°F
Humidity: 95%RH

- Viewing system requirement

Operating system

Microsoft Windows 98SE/ME/2000/XP

Browser

Internet Explorer 5.x or above

Electromagnetic Compatibility (EMC)

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

USA - This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a partial installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-- Reorient or relocate the receiving antenna.

-- Increase the seperation between the equipment and receiver.

-- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-- Consult the dealer or an experienced radio/TV technician for help.

Shielded interface cables must be used in order to comply with emission limits.

Europe CE - This digital equipment fulfills the requirement for radiated emission according to limit B of EN55022/1998, and the requirement for immunity according to EN50082-1/1992.

Liability

Vivotek Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Vivotek Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.